



Major Financial Institution Application Vulnerability Assessments

Assessments of online banking applications

Case Study

Challenge

Echelon IT Solutions staff have conducted a number of Application Vulnerability Assessments of the online banking application, as well as other internal and external facing applications for this major, 'top 6' Canadian bank. The scope of assessments have considered all application tiers, and included examination of JSP (Java Server Pages), Java Servlets, EJB (Enterprise Java Beans) and interfaces to various EIS (Enterprise Information Systems) back end, core systems.

Application Vulnerability Assessments conducted for the client consist of either one of, or generally, both of:

- Source Code Assessment – The detection of security vulnerabilities in the application through the examination of the application source code; and
- Runtime Vulnerability Assessment – The detection of security vulnerabilities in the application through the examination of the application in a runtime environment.

Source Code Assessment is a hands-on code review conducted by security analysts with significant programming backgrounds in the specific language. This approach allows Echelon to detect application vulnerabilities in a number of areas, including: input validation; initializations; authentication and authorization; auditing; confidentiality; coding practices and code quality, and auditing.

Using bankcard ids and user accounts provided by the client, as well as general anonymous access, a Runtime Vulnerability Assessment targets the application as it is deployed. Echelon security analysts: walk through typical usage scenarios for the application; identify key targets and assets; formulate and execute attack scenarios; and then harvest and assess the risk associated with the resulting findings. Attack scenarios and vulnerabilities examined include: SQL injection, broken authorizations, parameter manipulation; and incomplete enforcement of business rules. Preliminary findings and recommendations are formally reported throughout the assessment period and allow the client to quickly address any vulnerabilities detected.

The final assessment report presents all findings and recommendations from the application security vulnerability assessment. The report includes a qualitative risk assessment with recommendations for key findings and a detailed assessment with recommendations of all other findings. The comprehensive report details all findings, include those areas where sufficient security safeguards are detected.

The client has successfully integrated application security vulnerability assessments as part of its overall security program. Echelon has provided the professional assurance that the client needs to successfully manage its security risks.